International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 413– 417

Providing Data Security in Cloud Computing Using Elliptical Curve Cryptography

Ms. Priyanka Sharda
Department of Computer Engineering,
JD College of Engineering and Management
Email: priyankasharda10@gmail.com

Abstract- Cloud computing encourages IT organizations and providers to increase standardization of protocols and processes so that the many pieces of the cloud computing model can interoperate properly and efficiently. Cloud computing scalability is another key benefit to higher education, particularly for research projects that require vast amounts of storage or processing capacity for a limited time. Some companies have built Data Centres near sources of renewable energy, such as wind farms and hydroelectric facilities, and cloud computing affords access to these providers of ―green IT‖. Finally, cloud computing allows college and university IT providers to make IT costs transparent and thus match consumption of IT services to those who pay for such services. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Elliptic Curve Cryptography Algorithm provides secure message integrity and message authentication, along with non-repudiation of message and data confidentiality. Cloud Computing, the dream of computing as a utility, shifts user programs and data from personal computers to the clouds, providing all kinds of resources over the Internet.

Keywords:-*cloud computing, cloud security, data security, encryption, elliptic curve cryptography*.

*****

I. INTRODUCTION

A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand.

It allows people to do things they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology. Through cloud computing clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic.

The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud. Cloud storage services may be used through web service API or through web based user interface.

II. RELATED CONCEPTS ABOUT CLOUD

A. TYPES OF CLOUD MODELS

- **Public cloud**: the cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services.
- **Private cloud**: the cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.
- **Community cloud**: the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.
- **Hybrid cloud**: the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

B. CLOUD CHARACTERISTICS

- **On demand service**: cloud is large resource and service pool that you can get service or resource whenever you need by paying amount that you used.
- **Ubiquitous network access**: cloud provides services everywhere though standard terminal like mobile phones, laptops and personal digital assistants.
- **Easy to use**: the most cloud provider's offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.
- **Business model**: cloud is a business model because

it is pay per use of service or resource.

- **Location independent resource poling**: the providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand.

C. CLOUD DEPLOYMENT MODEL

- **Infrastructure as a service(IaaS):** it delivers a platform virtualization environment as a service rather than purchasing servers, software, data centers.
- **Software as a service (SaaS):** it is software that is deployed over internet and or is deployed to run behind a firewall in your LAN or PC.
- **Platform as a service(PaaS):** this kind of cloud computing provide development environment as a service

III. CLOUD SECURITY CHALLENGES

The cloud services present many challenges to an organization. When an organization mitigates to consuming cloud services, and especially public cloud services, much of the computing system infrastructure will now under the control of cloud service provider.

Many of these challenges should be addressed through management initiatives. These management initiatives will requires clearly delineating the ownership and responsibility roles of both the cloud provider and the organization functioning in the role of customer.

Security managers must be able to determine what detective and preventative controls exist to clearly define security posture of the organization. Although proper security controls must be implement based on asset, threat, and vulnerability risk assessment matrices. Cloud computing security risk assessment report mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud. Here are security risks list.

- Data segregation: data in the cloud is shared environment alongside data from other customers.
- Recovery: even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.
- Investigative support: investigating inappropriate or illegal activity may be impossible in cloud computing.

IV. PROPOSED SYSTEM: ECC ALGORITHM

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.
An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a

- characteristic that is very valuable for cryptography Regulatory compliance: cloud computing providers who refuse to external audits and security certifications.
- Privileged user access: sensitive data processed outside the organization brings with it an inherent level of risk.
- Data location: when you use cloud, you probably won't know exactly where your data hosted.

purposes: they are relatively easy to perform, and extremely difficult to reverse.

A: Grounds of Elliptic Curve

Elliptic curves has unique property that makes them suitable for use in cryptography i.e. it's ability to take any two points on a specific curve, add them together and get a third point on the same curve. The main operation involved in ECC is point multiplication, i.e. multiplication of a scalar K with any point P on the curve to obtain another point Q on the same curve.

An elliptic curve is defined by an equation, is of two variables, with coefficients. For the purpose of cryptography, the variable and coefficients are limited to a special kind of set called a FINITE FIELD. The general equation for an elliptic curve is:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where a, b, c, d and e are real numbers and x and y also take their values from real number. A simplified elliptic curve equation is given as:

$$y^2 – x^8 + dx + e$$

In Elliptical Curve Cryptography, the Elliptic Curve is used to define the members of the set over which the group is calculated i.e. an operation on any two elements of the set will give a result that is the member of the same set as well as operations between them which defines how math work in the group.

In real time situation the ECC is implemented over a finite prime field and in hardware, where binary number are used, the field is GF (2^m). The GF is a finite field namely Galois Field.

The field of finite primes provides the ECC that allows encipher to encrypt the data very easily but for the cryptologist the process of beginning to attack the encrypted message is very difficult.

The GF (p) is the field of integers module p, and consists of all the integers from 0 to p-1 in case of square graph, p*p in size, where p is a very large prime number.

To implement the ECC in software to handle prime numbers as well as other number, ECC allows the development of potable chips that can be deployed over the mobile devices and provide a suitable and processor friendly encryption . Like every other design consists of ECC that is implicated on hardware over binary finite fields, point adding and doubling on elliptic curve and scalar multiplication.

B. Curve Selection

To select a Curve, one of the following are the things to put into consideration as stated:

- The group order has to be first chosen. Since the criteria require knowing the group order, it is easier and faster to select that parameter first and then build a curve having that attribute.

- Use a known curve (possibly in other fields) to build a curve with the desired properties .This approach likely limits the number and the types of possible curves that can be produced, making it an advantage for the attacker.

- **Choose a random curve**: This is the slowest method. First coefficients are generated to make a valid elliptic curve, typically using a cryptographic random number generator. Then the number of points on the curve needs to be counted and factored. If one of the criteria is not satisfied, the values are discarded and start over. The algorithm used for counting points is Schoof's algorithm or the Schoof-Elkies-Atkin algorithm (SEA).

- **Use a published curve:** This is the easiest and fastest method. One concern is possible patent issues. Another is that the attacker may be more motivated to attack a publicly known curve since more people would use it. The chance of collision is also increased. Methods 1, 2 and maybe 4 likely produce curves with additional structure, which may be exploited by future mathematical advancements and discoveries. Although method 3 is slow, it is a better guard against future attacks on specific types of curves.

The components required for executing the task are as defined according to as follows:

• A prime number
• A point (with its components x and y) on a defined elliptic curve
• A scalar multiple

VII. PROPOSED ALGORITHM FOR DATA SECURITY USING ECC

Both clouds agree to some publicly-known data item.

a. The elliptic curve equation
   i. values of a and b
   ii. prime, p
b. The elliptic group computed from the elliptic curve equation
c. A base point, B, taken from the elliptic group

Key generation:

1. A selects an integer dA. this is A's private key.
2. A then generates a public key PA=dA*B
3. B similarly selects a private key dB and computes a public key
   PB= dB *B
4. A generates the security key K= dA *PB. B generates the secrete key K= dB *PA.

Signature Generation:

For signing a message m by sender of cloud A, using A's private key dA

1. Calculate e=HASH (m), where HASH is a cryptographic hash function, such as SHA-1
2. Select a random integer k from [1, n − 1]
3. Calculate r = x1 (mod n), where (x1, y1) = k * B. If r = 0, go to step 2
4. Calculate s = k − 1(e + dAr)(mod n). If s = 0, go to step 2

5. The signature is the pair (r, s)

6. Send signature (r, s) to B cloud.

Encryption algorithm:

Suppose A wants to send to B an encrypted message.

i. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic group.
ii. A chooses another random integer, k from the interval [1, p-1]
iii. The cipher text is a pair of points

PC = [(kB), (PM + kPB)]

iv. Send ciphertext PC to cloud B.

Decryption algorithm:

Cloud B will take the following steps to decrypt cipher text PC.

a. B computes the product of the first point from PC and his private key, dB
dB * (kB)
b. B then takes this product and subtracts it from the second point from PC

(PM + kPB) – [dB(kB)] = PM + k(dBB) – dB(kB) = PM

B cloud then decodes PM to get the message, M.

Signature Verification:

For B to authenticate A's signature, B must have A's public key PA

1. Verify that r and s are integers in [1, n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate w = s −1 (mod n)
4. Calculate u1 = ew (mod n) and
u2 = rw (mod n)
5. Calcúlate (x1, y1) = u1B + u2PA
6. The signature is valid if x1 = r(mod n), invalid otherwise.

B cloud then decodes PM to get the message, M.

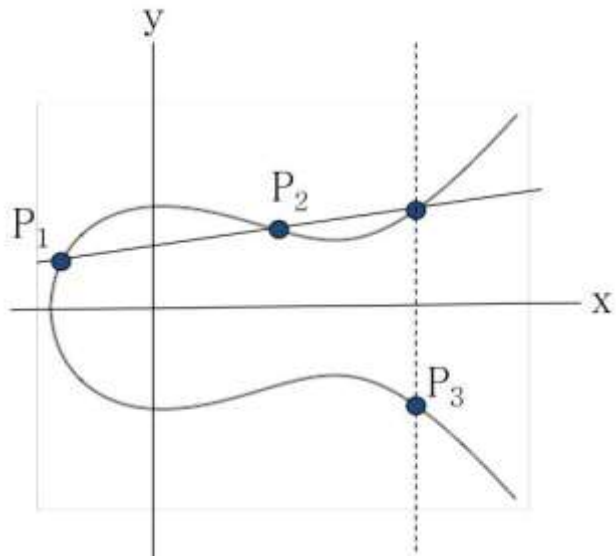
Signature Verification:

For B to authenticate A's signature, B must have A's public key PA

5. Verify that r and s are integers in [1, n − 1]. If not, the signature is invalid
6. Calculate e = HASH (m), where HASH is the same function used in the signature generation
7. Calculate w = s −1 (mod n)
8. Calculate u1 = ew (mod n) and
u2 = rw (mod n)

9. Calcúlate (x1, y1) = u1B + u2PA

The signature is valid if x1 = r(mod n), invalid otherwise.



As shown in picture. Let P1=(x1, y1), P2=(x2, y2), P3=(x3, y3) and P1 not equals P2

$$m = \frac{y_2 - y_1}{x_2 - x_1};$$

To find the intersection with E. we get

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

$$or, 0 = x^3 - m^2x^2 + \ldots$$

$$So, x_3 = m^2 - x_1 - x_2$$

$$\Rightarrow y_3 = m(x_1 - x_2) - y_1$$

V. CONCLUSION & FUTURE SCOPE

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques like RSA now in use. Although ECC's security has not been completely evaluated, it is expected to come into widespread use in various fields in the future. After comparing the RSA and ECC ciphers, the ECC has proved to involve much less overheads compared to RSA. The ECC has many advantages due to its ability to provide the same level of security .

The future of ECC looks brighter than other algorithms as today's applications (smart cards, pagers, and cellular telephones etc.) cannot afford the overheads introduced by RSA. At least, in today's small computing devices ECC can be used for encryption and decryption as it requires smaller key sizes and has lesser computing complexity as compared to other algorithms.

Thus, ECC makes it an ideal choice for portable, mobile and low power applications and their integration with cloud services. This work compares the time taken by the two algorithms for key generation and encryption. The importance of this work is to use ECC algorithm in cloud storage which has better security services. This work can be extended to compare ECC with other algorithms used for digital signatures, key exchanges as well as to provide the data integrity.

REFERENCES

[1] Alowolodu O.D, Alese B.K, Adetunmbi A.O., Adewale O.S ,Elliptic Curve Cryptography for Securing Cloud Computing Applications "*International Journal of Computer Applications (0975 – 8887)"* Volume 66– No.23, March 2013, pp 10-17

[2] Kangchan Lee, Security Threats in Cloud Computing Environments1,"*International Journal of Security and Its Applications* "Vol. 6, No. 4, October, 2012,pp 25-31

[3] Ravi Gharshi, Suresha, Enhancing Security in Cloud Storage using ECC Algorithm," *International Journal of Science and Research (IJSR)*" Volume 2 Issue pp 56- 64

[4] Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem, A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing " *IOSR Journal of Computer Engineering (IOSRJCE) ISSN : 2278-0661 ",*Volume 1, Issue 3 (May-June 2012), PP 28-36

[5] Dijk, Marten Van, and Ari Juels. "*On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing*." Computing 305 (2010): pp 1-8